Access Control in Geographic Databases

Liliana Kasumi Sasaoka[1] and Claudia Bauzer Medeiros[2]

[1] IBM Silicon Valley Lab
555 Bailey Ave, San Jose, CA 95141, USA
lilianas@us.ibm.com
[2] Institute of Computing, UNICAMP
13081-970 Campinas, SP Brazil
cmbm@ic.unicamp.br

Abstract. The problem of access control in databases consists of determining when (and if) users or applications can access stored data, and what kind of access they are allowed. This paper discusses this problem for geographic databases, where constraints imposed on access control management must consider the spatial location context. The model and solution provided are motivated by problems found in AM/FM applications developed in the management of telephone infrastructure in Brazil, in a real life situation.

1 Introduction

Security amd trust in databases are intimately associated with access control [AJS+96]. They determine *who* can access *what* data and *how*. In most cases, security models and mechanisms concentrate on low level system details, and do not consider semantics associated with the data. In particular, spatial applications present challenges not met by standard access control proposals.

Security issues are considered only at the implementation level, and not usually integrated into the modeling stage. Several access control models have been defined for relational or object-oriented databases. Specific models have also appeared – e.g., in the case of temporal [BJS95,BBF01] or video databases [BHAE00]. However, none of these mechanisms can be directly applied to geographic applications, because of their particular characteristics. Indeed, when attribute semantics are associated with the spatial localization, data management demands distinct types of control, which has to be defined in terms of geographic region. In other words, access control becomes spatially sensitive.

Consider the following scenario, which will be used throughout the paper to motivate our solution. A utility (telephone) company wants to develop a GIS project that concerns infrastructure expansion in a city, for a specific geographic region R. Several engineers and experts will be concerned – they work cooperatively in the expansion planning for R, having distinct needs and authorizations for data access. At the same time, normal operations proceed (e.g., repairs and maintenance) and other people will have access to data on the same region, again with distinct permissions. Whereas standard access control proposals concern only thematic data, spatial access control involves issues such as “John can only update data concerning the area within blocks A and B", or "Repairs recorded for an area X will override any other operations being requested for this area". It must furthermore be possible to grant access only for one spatial object (a pole), a set of objects (e.g., poles in a street), or a neighborhood.

A specific system that demands this kind of geographic access control is the Brazilian CPqD Outside Plant Management System, formerly known as the SAGRE System [Mag97]. It is an integrated set of GIS-based software applications to manage the expansion, modernization and operation of an outside telephone plant. Used throughout Brazil by major telephone companies, it has very large geographic databases for most of Brazil's major cities, and hundreds of thousands of lines of code.

SAGRE has been in operation and continuous evolution since the beginning of the nineties. It is used in several sectors of telecom companies, by people with different roles. This gave rise to the need to control access to the operations that use its database taking spatial information into account.

Our paper shows how to solve this problem by extending classical models and mechanisms to the spatial context. Though our solution is general, it was motivated by the needs of the CPqD Outside Plant Management System.

The rest of this paper is organized as follows. Section 2 introduces related work. Sections 3, 4 and 5 describe our model and access control mechanism. Section 6 presents the access control problems in SAGRE and discusses the use of the proposed mechanism in this context. Finally, section 7 presents conclusions and possible extensions.

2 Basic concepts and related work

2.1 Authorization models

All access control mechanisms are based on some authorization model, which defines how a database management system must implement access control. It is generally composed by: (i) access granularity indication; (ii) structures to represent the authorization (formal semantics of representation); (iii) a set of policies to manage and to grant authorizations; and (iv) algorithms to analyze access requests based on the existing authorizations.

Access *granularity* defines the storage unit to control data access – e.g., at the tuple, tables or databases levels. The most common *authorization structure* is represented by the triple $<s, o, m>$, where: s is the subject who receives the authorization, o the object which is authorized and m the access mode.

Objects o are the passive entities storing information, such as tables, tuples, or even elements of a tuple. Subjects are active entities that access the objects and can be users, user groups or processes operating on behalf of users. The subject can also be defined in terms of roles.

The m in $<s, o, m>$ corresponds to the access mode – i.e., the type of operation that the subject has permission to execute on the object. [BDPSN96] defined the basic set of operations as: read, write, delete, execute and create. Authorizations can be further refined into positive or negative (forbidden).

The set of *policies* to manage authorizations are rules that define: who will grant and revoke permissions (e.g., owner, administrator, any user), operations authorized (e.g., read, write), and how these will be executed. Policies also define factors such as negative authorizations and authorization derivation.

Finally, in order to have a complete authorization model, one must also define *mechanisms* or *algorithms* to validate an access request based on the stored authorizations. As will be seen, the mechanism we propose specifies all the required model components: granularity, structure, policies and algorithms.

2.2 Access control mechanisms

Current research efforts on access control can be classified in three main directions [BDPSN96]: Discretionary Access Control (DAC), Mandatory Access Control (MAC) and the combination of both, the Role Based Access Control (RBAC). Efforts normally are defined in terms of the $<s,\ o,\ m>$ structure.

DAC is based on granting and revoking privileges [GW76]. Discretionary protection policies govern the access of users (the subjects) to the information, on the basis of the users identity and the rules that specify, for any user and any object in the system, the types of accesses allowed. A subject's request to access an object is checked against the specified authorizations; if there exists an authorization stating that the subject can access the object in the specific mode, the access is granted; otherwise, it is denied. Policies are discretionary: they allow subjects to grant other subjects authorizations to access the objects.

MAC is based on classifying subjects and objects of the system in hierarchical levels, satisfying the requirements of military, governmental and commercial organizations [BJS95]. This hierarchical organization assures that classified information does not flow to lower levels. It is based on two principles formulated by Bell and LaPadula [BP76]. The first states that no subject can read an object of an upper level. The second does not allow a subject to write in an object of a lower level, ensuring that no information will flow from upper to lower levels.

Access decisions on the Role Based Access Control (RBAC) [FK92] are based in the roles that a user can perform inside an organization. This adds flexibility to access grants, which become context-sensitive.

New devices and applications have given rise to other kinds of concerns. The Web has motivated research on adaptations of RBAC to this new environment (e.g. [PSA01]), and studies on distinct granularity levels for protection of XML documents [BCFM00]. The field of sensor networks has prompted studies on coordination and fusion of sensor data, and protocols for access control to save energy (e.g., [WHE04]).

Few authors are concerned with the special needs of spatial access control. The work of [BBC^{+}04] proposes a discretionary model that considers, among others, derivation of authorization rules, privilege propagation and negative authorizations over vector data. This work is extended to a model called GEO-RBAC, which considers RBAC in the spatial context [BCDP05]. This model is motivated by the needs of location-based services and mobile applications. It provides flexibility in access specification, associating roles with a spatial context and changing authorizations according to spatial granularity. Roles are instances of a role schema; authorizations can be globally assigned to all roles in a schema, or be refined for a specific role. Roles are "activated" according to a subject's location.

As will be seen, the main differences between these two proposals and our model are the fact that we were motivated by the needs of cooperative work in spatial applications, for a very large real GIS application. As a consequence, some aspects of our solution are concerned with simplifications for performance reasons, and specific user needs. Roles are defined by user groups.

3 Authorization model for geographic data

This section presents the main components of our model: granularity, subject, object, access mode, adopted authorization rules, policies and algorithms.

Definition - Spatial authorization rule A spatial authorization rule is defined by the triple $< s, o, m >$, where s is the authorized subject; o the set of authorized objects and m, the access mode. The object o can be represented by identifiers (explicit ennumeration) or by a spatial query (implicit specification). Queries are discussed in section 5. The access mode can be read or write.

3.1 Stating and storing an authorization rule: s, o, m

We assume that all spatial data are stored in a spatial database, accessed by a GIS. Moreover, this database also contains a special repository with the authorization rules (referred to as "rule database"), which specify spatially-dependent access control. We use a simplified spatial data model, based on OGC's, which is sufficient for the purposes of our explanation. We consider that data in geographic databases can be characterized as having two types of attributes: descriptive and spatial features. This research is limited to vector data, geometries being classified into three types: point (e. g., a pole), line (e. g., a street), or polygon (e. g., a parcel).

From a high abstraction level, an authorization process can be understood as being defined according to the following sequence of stages: (1) definition of authorization rules, (2) mapping of these rules into some set of database structures and (3) definition of a rule management mechanism.

In our context, the first stage – definition of authorization rules – is specified as:

[Define $<s,\ m>$ on $<o>$], where $<o>$ is a result of a spatial query.

An authorization can be granted to an individual user, groups of users or user roles associated with different operations. Object $<o>$ defines a data partition within the database for which that authorization holds. It can be a spatial component or a set of components, with geometries of type polygon, point or line, and be directly specified (through identifiers), or indirectly, as a query result.

A spatial permission is therefore directly related to the spatial query that it must satisfy. For example, the authorization "Ann has read access to all the rivers in São Paulo state" is nothing more than a read permission to access all data on rivers resulting from the spatial query "select all the information of river features in São Paulo state" – see Section 5.

Subjects s can be defined in the same way as in conventional databases. The model considers that subjects are end users – engineers and designers within an AM/FM planning environment: their roles are indirectly defined by their login group. This is a compromise between full RBAC and DAC. This can easily be extended to include explicit roles, or software.

3.2 Granularity

Access granularity in our rules is that of the objects they define. This requires considering trade offs between number of objects considered in a rule and increased system complexity – the number of rules in the rule database increases with smaller access granularity. Similar to [BCDP05], we support hierarchical definitions of spatial extent, which is used to infer non-explicit rules.

Our solution considers two authorization rule specifications: $< s, o, m >$ and $< s, Q, m >$. The first one explicitly references the object identifier (for example, a point related to a specific pole, a line related to a street, a polygon related to a neighborhood). In this case, the authorization is executed in an individual object in the database. The second specification contains a spatial query, which defines the objects under control (see section 5). This solution is a compromise between management of specific objects ($< s, o, m >$ rules) versus flexibility in defining authorizations ($< s, Q, m >$ rules).

Consider the following rule: "Ann has read access to Jardim Paulista neighborhood", where object "Jardim Paulista" is a polygon identified by [id 501] – its geometry defines access granularity. The rule which is going to be stored is $< Ann, 501, read >$ – Ann is allowed access to object 501 and all the objects inside 501 (see section 5).

A rule example using a query and with point granularity is "John can access just the subway stations in Vergueiro Street", where subway stations are points in the street. In this case, the rule is (John, all the subway stations in Vergueiro Street, read), where "all the subway stations in Vergueiro Street" can be specified as a spatial SQL query.

3.3 Set of policies to manage and administer authorizations

The model proposes a centralized administration of authorizations: just the administrator can grant and revoke permissions. Thus, it is not necessary to worry about the cascade and non-cascade revocation of authorizations, as in the DAC model [GW76].

Our model does not consider negative authorizations. These must be analyzed according to the application, and introduce a major complexity in the algorithms that evaluate an access request. If the mechanism allows negative authorizations, given an access request, it is necessary to verify if there are negative authorizations denying the use of an object, before allowing the access.

3.4 Algorithms to analyze access requests

As mentioned before, our access control mechanism assumes that authorization rules are stored in a special repository within the database, and checked at access request. This request can be per transaction, or apply to an entire user session, and assumes that all the rules stored in the database are consistent according to the policies defined by the administrator. Access right is only granted if there is an explicit rule authorizing the subject to access that object with that access mode, or if the user access grant can be inferred using spatial containment properties.

Algorithm Access request validation
Input:
[1] access request (S, Q_a, M).
[2] set of database authorization rules (s, o, m) and (s, Q, m), stored in the rule repository
Output: [1] AUTHORIZED or [2] DENIED

1. Given an access request $AR = < S, Q_a, M >$ where the query statement Q_a defines objects to be accessed, select all authorization rules $r_i = < s, o, m >$ and $r_j = < s, Q_j, m >$ from the rule database, where $s = S$ and $m = M$. The result of this step is a set of rules $RA = \ < S, o_i, M > \bigcup < S, Q_i, M >$.

2. Process the queries Q_i in $< S, Q_i, M >$ in order to determine the referenced objects, obtaining the final set of rules $RF = \ < S, o_k, M >$, where o_k are the objects returned by the execution of all Q_i queries.

3. Process the query Q_a, getting $AR = \ < S, o_a, M >$, which determines the objects involved in the access request.

4. Detect conflicts between AR and objects in RF, according to section 4.

5. Resolve the conflicts using the policies defined in section 4.

Details of steps 4 and 5 can be found in [Sas02].

4 Managing conflicts for geographic access control

Access conflicts require checking spatial relationships between access requests and rules in the database. Generally speaking, conflicts fall into two cases: (i) objects totally or (ii) partially contained in another.

In case of total containment, access is granted, according to inference rules for hierarchies of objects subject to total containment. The existence of authorization $< s_1, o_2, m_1 >$ allows to infer $< s_1, o_1, m_1 >$, if o_1 is totally contained in o_2.

Partial containment, however, introduces conflicts. Again, suppose s_1 has access to o_2, and that object o_1 is partially contained in o_2. Should s_1 be granted access to o_1? In this case, there are the following alternatives, which are considered at step 4 with possible user disambiguation:

1. yes, s_1 can access object o_1, even if it is partially contained in o_2;

2. s_1 can access the part of the object o_1 contained in o_2. This requires cutting the object in parts;
3. yes, only if there is also an authorization rule $< s_1, o_1, m_1 >$, which authorizes s_1 to access the object o_1 explicitly;
4. yes, only if there is also an authorization rule $< s_1, o_3, m_1 >$ in the database, where o_3 contains the rest of o_1 not contained in o_2;
5. yes, s_1 can access o_1, if there is no negative authorization $< s_1, o_1, m_1, - >$;
6. no, the situation does not occur because objects partially contained in another do not exist in the application domain.
7. no, the access to objects partially contained in another is denied.

5 Spatial queries for access control

The spatial attributes considered in this research for access control are of type point (e.g., poles, trees), lines (e.g., street segments) and polygon (e.g., neighborhoods). The type depends on the scale. For example, in a 1:1.000.000 scale, cities, small woods and many types of surfaces can be represented by points.

ueries for access control involve different relationships between spatial object types (e.g., Point x Point, or Line x Line). They return a result set, which is the target of access control, the object o of the $< s, o, m >$ triple. Different types of permission can be associated with each query result. We consider topologic and metric spatial query predicates and adopt the five topological operators defined by Clementini et. al. [CdFvO93] – in, overlap, touch, cross and disjoint – as sufficient to cover binary topological relationships.

The study of the objects in the database for access control must take two factors into account: (1) the result - spatial object, non-spatial object or part of an object; and (2) the predicate - spatial, non-spatial or both. Queries can produce descriptive or spatial attributes, or both. Query Q_x "Who are the subscribers recorded in the database" returns non-spatial objects (subscribers). The query Q_y "Which are the types of the cables installed in the Cambuí neighborhood" returns descriptive attributes (types of cable) for a spatial object (cables). The query Q_z "Supermarkets with more than 5 telephones installed" returns spatial objects (supermarkets), assuming that they have a spatial component. Query Q_x uses non-spatial predicates, while query Q_y uses a spatial predicate.

Consider query Q_z "Supermarkets with more than 5 telephones installed". An example of an authorization rule involving Q_z might be "Ann can update the account charges data of the supermarkets with more than 5 telephones installed", where s: Ann; o: points (supermarkets); m: write; the predicate is defined on descriptive attributes (number of telephones in a supermarket).

This type of reasoning, separating the definition of the permission from that of objects subject to access control, can be repeated for combinations of spatial objects and distinct predicates, and involve distinct kinds of geometric features.

6 Access control in SAGRE

As mentioned in section 1, our work was motivated by the need for spatially sensitive access control for cooperative work in the CPqD Outside Plant Management System. This system will be referred to in the rest of this section by its ancient name – SAGRE – to disambiguate references to the system and to its modules (see [Sag] for a description of the main functionalities of the system). It is a GIS-based system composed by a set of applications which automate processes related to outside telephone plant management. Two of its applications are relevant to access control issues: *Adm* and *Cad*.

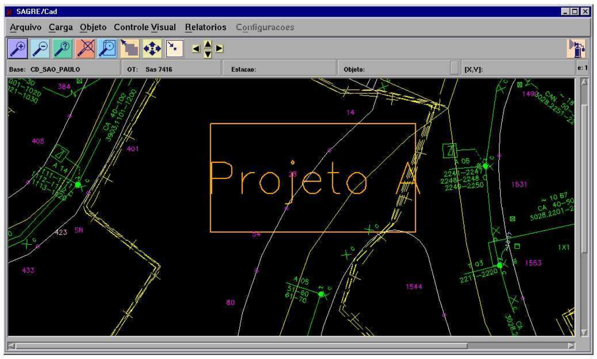
The Adm application is geared towards system administrators in telecom companies. It allows managing the system users, and groups, inserting and deleting users, granting and revoking role permissions for users/groups.

The Cad application maintains the basic urban map and the telephone outside plant. The basic urban map [Mag97] is composed by the urban planning basic elements, such as: streets, street segments, monuments. The outside plant corresponds to the infrastructure information used by telecommunications services such as poles, terminal boxes, cables. The Cad application supports the management of projects, where a "project" involves infrastructure maintenance or expansion planning for a given region, usually within some urban area. When creating projects, it is necessary to indicate a manager and the manager's area using geographic coordinates, defined as a polygon.

Our first modification concerns the Adm application, changing the internal tables that store user roles. They must contain insert, update and delete authorization rules that indicates the spatial element o, which will be authorized. User authentication must also be changed, since it will pass through more verification stages. Project managers can also intervene here.

Figure 1 presents a screen copy with a project developed using Cad. In normal system usage, a user has to define the geographic limits of a project (a polygon). Notice the area covers parts of features (e.g., lines), which complicates access control. The polygon is only used for visualization and does not impose any restrictions on objects to be modified by this project. The present version of Cad contains special code that verifies some spatial access control, but it is not flexible enough to consider different situations. An example of such a problem is the case of update cascades, where an update in a given object may propagate to objects outside the visible polygon. Thus, a person within a project confined to this polygon can change objects even when they are outside the project polygon.

This means that changes must be made to allow preprocessing access requests. Even though some of our solutions have been considered in SAGRE, their full-fledged implementation would require a new module - Geographic Access Manager - to be created to check and manage spatial access rules [Sas02]. The generic solution, using authorization rules in a database and distinct kinds of access modes, still needs to be taken into account. Visualization must also be restricted to prevent users from seeing certain objects.



Base: CD_SAO_PAULO

OT: Sas 7416

Estacao:

Objeto:

[X,Y]:

Fig. 1. Project designed in SAGRE/Cad.

7 Conclusions and extensions

This paper presented a generic access control model for GIS applications. The proposal is based on the definition of authorization rules $< s, o, m >$, where objects o are characterized as a result of a geographic query. The main contributions of this paper are: survey of requirements for access control in geographic databases; definition of an authorization model based on the spatial characterization; discussion of implementation aspects of this model; brief presentation of application of the proposed mechanism for a real GIS system.

Spatially-sensitive access control is a research area that presents several challenges, with relatively few papers on the subject – e.g., [BCDP05,BBC+04]. The main differences with our proposal were that we were forced to simplify some of the issues, given the size and scope of SAGRE and its multiple user roles – e.g., we do not consider negative permissions, and roles are defined by login groups. Moreover, our proposal is geared towards solving problems that arise in cooperative planning activities using a GIS, while at the same time allowing normal operation for the same region.

Many extensions can be proposed. One concerns spatio-temporal access control. Another possibility is the incorporation of nested permissions. Also, conflicts among our rules must be studied, to maintain rule consistency. We have made a preliminary study concerning performance impact of our rule checking algorithms. Further work must be conducted along these lines.

Acknowledgements This work was partially financed by CPqD Telecom & IT Solutions, CNPq, FAPESP, CNPq SAI, Agroflow and Web-MAPS Projects.

References

[AJS+96] V. Ashby, S. Jajodia, G. Smith, S. Wisseman, and D. Wichers. Trusted Database Management Systems - Interpretation of the Trusted Computer

System Evaluation Criteria. Technical Report 001-005, National Computer Security Center, 1996. 75 pages.

[BBC$^+$04] A. Belussi, E. Bertino, B. Catania, M. Damiani, and A. Nucita. An Authorization Model for Geographical Maps. In *Proc. 14th ACM GIS*, pages 82–91, november 2004.

[BBF01] E. Bertino, P. Bonatti, and E. Ferrari. TRBAC: Temporal Role-Based Access Control Model. *ACM Transactions on Information and System Security*, 4(3):191–223, 2001.

[BCDP05] E Bertino, B. Catania, M. Damiani, and P. Perlasca. GEO-RBAC: a spatially aware RBAC. In *Proc, 10th ACM Symposium on Access Control*, pages 29–37, june 2005.

[BCFM00] E. Bertino, S. Castano, E. Ferrari, and M. Mesiti. Specifying and enforcing access control policies for XML document sources. *World Wide Web*, 3(3):139–151, 2000.

[BDPSN96] A. Baraani-Dastjerdi, J. Pieprzyk, and R. Safavi-Naini. Security in Databases: A Survey Study. February:1–39, 1996. *http://citeseer.nj.nec.com/baraani-dastjerdi96security.html*.

[BHAE00] E. Bertino, M. A. Hammad, W. G. Aref, and A. K. Elmagarmid. An access control model for video database systems. In *CIKM*, pages 336–343, 2000.

[BJS95] E. Bertino, S. Jajodia, and P. Samarati. Database Security - Research and Practice. *Information Systems*, 20(7):537–556, 1995.

[BP76] D. E. Bell and L. J. La Padula. Secure Computer Systems: Unified exposition and Multics interpretation. Technical report, The Mitre Corp., 1976.

[CdFvO93] E. Clementini, P. di Felice, and P. van Oosterom. A Small Set of Formal Topological Relationships Suitable for End-User Interaction. *Proceedings of the* 3rd *Symposium Spatial Database Systems*, pages 277–295, 1993.

[FK92] D. Ferraiolo and Richard Kuhn. Role-Based Access Control. *Proceedings of* 15th *National Computer Security Conference*, 1992.

[GW76] P. G. Griffiths and B. Wade. An authorization mechanism for a relational dabase system. *ACM TODS*, 1(3):243–255, 1976.

[Mag97] G. C. Magalhaes. Telecommunications outside plant management throughout Brazil. In *Proc GITA 1997*, 1997.

[PSA01] J. Park, R. Sandhu, and G. Ahn. Role-Based Access Control on the Web. *ACM Transactions on Information and System Security*, 4(1):37–71, 2001.

[Sag] Sagre. http://www.cpqdusa.com/solutions/outside.html, accessed on April 2006.

[Sas02] L. K. Sasaoka. Access Control in Geographic Databases. Master's thesis, Universidade Estadual de Campinas, June 2002. In Portuguese.

[WHE04] W.Ye, J. Heidemann, and D. Estrin. Medium Access Control with Coordinated Adaptive Sleeping for Wireless Sensor Networks. *IEEE/ACM Transactions on Networking*, 12(3):493–506, 2004.